QUANTENCOMPUTING

Algorithmen für neue Hardware

Quantenalgorithmen lösen nur bestimmte Rechenprobleme signifikant effizienter als klassische Algorithmen.

Mario Berta

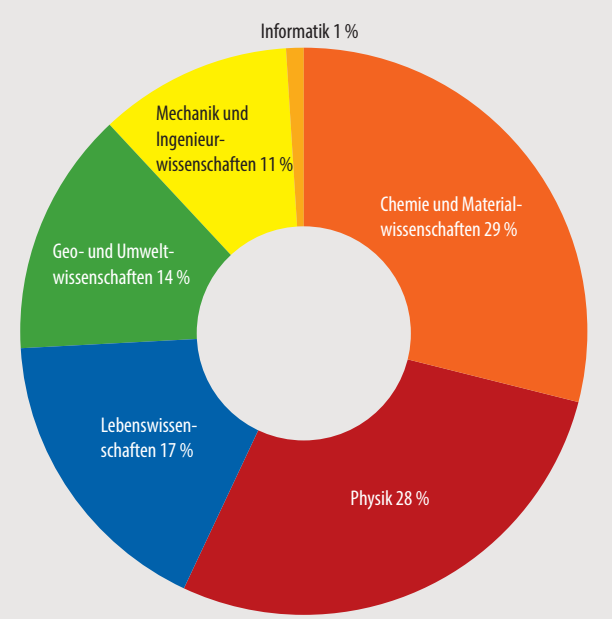
Bei der Lösung gewisser rechenintensiver Probleme könnten neuartige Computer mit quantenmechanischen Hardware-Elementen effizienter arbeiten als klassische Supercomputer. Forschungsteams aus Wissenschaft und Industrie suchen nach praxisrelevanten Quantenvorteilen und passenden Quantenalgorithmen.

Computer werden jedes Jahr leistungsstärker: Nach dem Mooreschen Gesetz verdoppelt sich seit den 1970er-Jahren die Anzahl der Transistoren auf einem Prozessor ungefähr alle zwei Jahre. Weil damit eine exponentielle Verkleinerung der einzelnen Bausteine einhergeht, zeigen sich mittlerweile quantenmechanische Effekte. Die grundlegende Idee von Quantencomputern ist es, solche Quanteneffekte nicht wie beim modernen Chipdesign zu minimieren, sondern diese kontrolliert einzusetzen, um konzeptuell neue Rechenschemata zu ermöglichen.

Schon in den 1980er-Jahren brachte Richard P. Feynman erstmals die visionäre Idee auf, mikroskopisch kleine Systeme wie einzelne Moleküle mit quantenmechanischen Chips anstelle von klassischen Computern zu simulieren [1]. Konkrete effiziente Algorithmen für solche Quantenchips waren jedoch zu dieser Zeit noch nicht bekannt. Rund zehn Jahre später hat Peter W. Shor einen Quantenalgorithmus für ein anderes Problem präsentiert: die Primfaktorzerlegung. Der Shor-Algorithmus zeigte erstmals einen klaren komplexitätstheoretischen Quantenvorteil gegenüber den besten bekannten Algorithmen für klassische Computer [2].

Seither hat sich die Idee von Quantencomputern als eigenständiges, interdisziplinäres Forschungsgebiet etabliert und weltweit zu Investitionen in diese Wissenschaft geführt. In den 2010er-Jahren haben viele große Technologiekonzerne eigene Forschungsteams aufgebaut. Spätestens seit 2019 das Team von Google Quantum AI verkündete, experimentell eine „Quantum Supremacy“ erreicht zu haben [3], kam es zu einem regelrechten Hype. Dazu gehören unter anderem vage versprochene Anwendungen in der Wissenschaft, wie die computergestützte Entwicklung von Materialien oder Arzneimitteln.

Der folgende Beitrag diskutiert kritisch, wie Quantenalgorithmen funktionieren und was sie von klassischen Algorithmen unterscheidet. Er stellt vielversprechende Anwendungsgebiete vor und erklärt, wie sehr sich die Quantenhardware noch verbessern muss, um für bestimmte Probleme wirklich konkurrenzfähig mit klassischen Supercomputern zu werden.



Swiss National Supercomputing Centre

Das Beispiel des Swiss National Supercomputing Centre zeigt, dass die Simulation von Quantensystemen viel Rechenzeit beansprucht. Quantencomputer könnten hier effizienter arbeiten.

Die Effizienz von klassischen und Quantenalgorithmen lässt sich mit einem Komplexitätstheoriemodell vergleichen, das die Anzahl elementarer Rechenoperationen zählt, die nötig sind, um ein gewisses Problem zu lösen. In der klassischen Welt stellt ein Bit die grundlegende Informationseinheit dar. In allgemeinen Algorithmen, die auch Zufälligkeit als Ressource verwenden, nimmt das Bit mit gewissen Wahrscheinlichkeiten die Werte 0 und 1 an. Die Komplexität eines klassischen Algorithmus ergibt sich aus der Anzahl benötigter Bits sowie der Anzahl benötigter elementarer Rechenoperationen, zum Beispiel der Addition zweier Bits.

Im Gegensatz dazu ist die elementare Informationseinheit in der Quantenwelt das Quantenbit bzw. Qubit, das mathematisch als Vektor auf der Einheitskugel beschrieben wird (**Abb. 1**). Elementare Rechenoperationen entsprechen Rotationen dieses Vektors sowie entsprechenden Transformationen auf zwei Qubits. Analog zum klassischen Modell folgt die Komplexität aus der Anzahl Qubits und der Anzahl elementarer Rotationen, die nötig sind, um ein gewisses Problem zu lösen. Dieses Quantengattermodell hat

den Vorteil, unabhängig von den Details einer bestimmten Implementation zu sein. So erlaubt es, die Komplexität von Algorithmen direkt auf abstraktem Level zu quantifizieren.

Im Quantengattermodell nimmt ein Quantenalgorithmus eine allgemeine Struktur an (**Abb. 2**): In einem einfachen Beispiel erfolgt zunächst die Initialisierung zweier Qubits im Grundzustand $|0\rangle$. Anschließend kommt es zu Rotationen der einzelnen Qubits sowie entsprechenden interagierenden Rotationen auf beiden Qubits. Das Auslesen der Resultate ergibt sich aus der Messung, die für jedes Qubit probabilistisch einen Wert von 0 oder 1 liefert. Dementsprechend ist das klassische Resultat eines Quantenalgorithmus eine Wahrscheinlichkeitsverteilung über Bitfolgen, was analog zu einem klassischen probabilistischen Algorithmus ist. Der wesentliche Unterschied besteht nun darin, wie der Quantenalgorithmus zum Resultat kommt. Die neu gewonnene Freiheit von komplexen Amplituden in den Quantenzuständen ermöglicht das Ausnutzen konstruktiver Interferenzen in den Rechenschritten, welche mit klassischen Algorithmen nicht zugänglich sind. Dies ist der exakte mathematische Grund für mögliche Quantenvorteile.

Um zum Beispiel eine Zahl mit n Stellen als Produkt von Primzahlen zu schreiben, braucht der effizienteste klassische Algorithmus etwa $2^{n^{1/3}(\log n)^{2/3}}$ elementare Operationen. Der Shor-Algorithmus kommt dagegen mit $n^2 \log(n)$ elementaren Quantenoperationen aus. Da die klassische Komplexität fast exponentiell mit n wächst, während die Quantenkomplexität nur etwa quadratisch mit n skaliert, ist die Primfaktorzerlegung für sehr große n nach heutigem Wissensstand nur mit Quantencomputern möglich, sobald entsprechend gute Quantenhardware existiert.

Zur Komplexitätstheorie

Der Shor-Algorithmus für die Primfaktorzerlegung stellt nach wie vor das beste Beispiel eines algorithmischen Quantenvorteils dar. Nach 30 Jahren intensiver Forschung an der Grenze zwischen klassischen und Quantenalgorithmen gibt es heute ein stark verbessertes komplexitätstheoretisches Verständnis, welche Quantenvorteile theoretisch möglich sind und wo klassische Supercomputer besser bleiben.

Im Allgemeinen scheinen kleinere Quantenvorteile, sogenannte quadratische Verbesserungen, generisch möglich zu sein. Für größere Quantenvorteile bedarf es dagegen einer speziellen Struktur im zugrundeliegenden Problem [4]. Außer spezifischen Rechenproblemen, wie der Primfaktorzerlegung mit versteckten zahlentheoretischen Symmetrien, betrifft dies vor allem physikalisch inspirierte Strukturen, sodass aus komplexitätstheoretischer Perspektive die Simulation von quantenmechanischen Systemen und deren Eigenschaften vielversprechend erscheinen. Dies gilt insbesondere für Probleme der Physik der kondensierten Materie oder der Computerchemie bei der Simulation von Molekülen. Potenzielle industrielle Anwendungen finden sich zum Beispiel in der computergestützten Entwicklung von Materialien oder Arzneimitteln.

Ein konkretes Beispiel ist die Simulation, wie sich n-Teilchen-Quantensysteme in der Zeit entwickeln. Ausgehend von einem effizient zu präparierenden Anfangszustand $|\psi(0)\rangle$ ist es das Ziel, den zeitentwickelten Zustand $|\psi(t)\rangle = \exp(-iHt)\,|\psi(0)\rangle$ zu erreichen, wobei die Hamilton-Matrix H das Zusammenspiel der n Teilchen modelliert. Da Interaktionen in der Physik typischerweise lokal stattfinden, lässt sich die $2^n \times 2^n$-große Hamilton-Matrix als Summe von „polynomial in n"-vielen Pauli-Matrizen schreiben, die sich wiederum mit nur polynomial vielen nativen Quantengattern $\exp(-iHt)$ implementieren lassen [1, 5]. Im Gegensatz dazu ist es im Allgemeinen unklar, ob und wie klassische Methoden diese physikalische Struktur einer dünn besetzten $2^n \times 2^n$-großen Hamilton-Matrix in der Pauli-Basis ebenso effizient ausnützen könnten. Schlussendlich bleibt die Frage, was über den zeitentwickelten Zustand $|\psi(t)\rangle$ mittels Messungen auslesbar ist. Dies führt übrigens zu weiteren Kosten, die es gegenüber klassischen Methoden auszuwerten gilt [6].

Für den heutigen Stand ist aber auch entscheidend, dass die genaue Untersuchung von Quantenalgorithmen für allgemeine Rechenprobleme aus der linearen Algebra oder der Optimierungstheorie auch zu einem Fortschritt auf der klassischen Seite geführt hat. Genauer gesagt hat sich gezeigt, dass randomisierte klassische Algorithmen für die meisten generisch rechenintensiven Probleme ohne physikalische Struktur ähnlich effizient funktionieren können wie entsprechende Quantenroutinen [7]. Dies betrifft

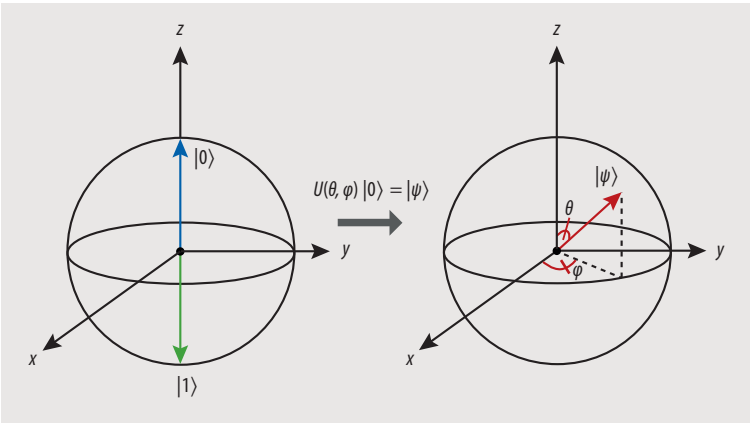


Abb. 1 Die Bloch-Kugel stellt Qubit-Zustände graphisch dar: Sie entsprechen allgemein Punkten mit $|\psi\rangle = \cos(\theta/2)\,|0\rangle + \exp(i\varphi)\sin(\theta/2)\,|1\rangle$, während sich die klassischen Zustände $|0\rangle$ und $|1\rangle$ auf die z-Achse beschränken.

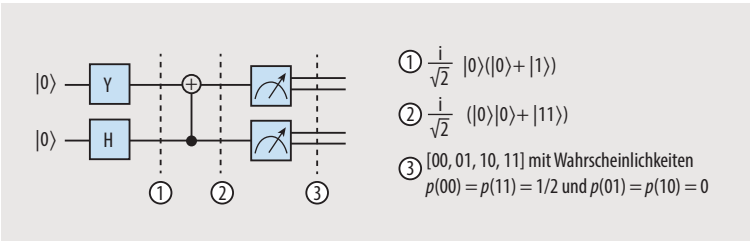


Abb. 2 Zu Beginn sind beide Qubits im Grundzustand $|0\rangle$ initialisiert. Die elementaren Rechenschritte entsprechen Rotationen auf der Bloch-Kugel: Auf das erste Qubit wirkt ein Pauli-Gatter Y, auf das zweite ein Hadamard-Gatter H, sodass der Zustand $|0\rangle|0\rangle = i/\sqrt{2}\cdot|1\rangle(|0\rangle+|1\rangle)$ resultiert. Anschließend lässt ein CNOT-Gatter die beiden Qubits durch eine globale Rotation miteinander interagieren, bevor Messungen das Ergebnis in klassische Bits überführen.

insbesondere diverse vorgeschlagene Anwendungen im Bereich des maschinellen Lernens oder des Finanzwesens. Obwohl das letzte Wort hier wohl noch nicht gesprochen ist, bleibt es wünschenswert, dass die Industrie von einem universellen Wunschdenken wegkommt und die konkreten wissenschaftlichen Fortschritte der letzten Jahre kritisch in Diskussionen miteinbezieht. Jede Woche erscheinen spannende, neue Ideen zu Quantenalgorithmen. Aus theoretischer Sicht gilt es aufzulösen, welche Routinen sich auch klassisch effizient emulieren lassen und für welche sich Quantenalgorithmen lohnen.

Fehlerbehaftete Quantencomputer

Neben den diskutierten komplexitätstheoretischen Betrachtungen stellt sich die ebenso grundlegende Frage, ob das abstrahierte Quantengattermodell auch physikalisch umsetzbar ist. Unabhängig von der verwendeten Hardware sind quantenmechanische Zustände von Natur aus sehr fragil, sodass sich schnell Fehler einschleichen. Zum Beispiel kann ein Qubit, das sich während der Laufzeit eines Quantenalgorithmus im angeregten Zustand $|1\rangle$ befindet, spontan zurück in den Grundzustand $|0\rangle$ fallen und so zu falschen Endresultaten führen.

Die heutige Generation von Quantencomputern arbeitet mit der Größenordnung von hundert physikalischen Qubits, deren Konnektivität untereinander eingeschränkt ist; sie kann elementare Rechenoperationen mit Fehlern im Bereich von 10^{-2} bis 10^{-5} ausführen. Dies entspricht nicht dem theoretischen Quantengattermodell, das von fehlerfreien Qubits, fehlerfreien Quantengattern und beliebiger Konnektivität ausgeht. Ohne weitere Maßnahmen führen die Fehlerraten automatisch dazu, dass maximal 10^2 bis 10^5 elementare Rechenoperationen ausführbar sind, bevor nur noch Rauschen vorliegt. Obwohl im algorithmischen Bereich momentan viele Publikationen zu fehlerbehafteten Quantencomputer entstehen und interessante Routinen, zum Beispiel für die Abschwächung von Fehlern [8] oder zu Quantensoftware entwickelt werden, bleibt unklar, ob es bereits skalierbare und potenziell nützliche Quantenvorteile geben kann. Auch wenn die verkündete „Quantum Supremacy“ mit fehlerbehafteten Quantenprozessoren zustande kam [3], ergibt sich daraus noch kein Quantenvorteil für wissenschaftlich oder industriell interessante Probleme. Für anwendungsrelevante Probleme gibt es diverse Abschätzungen, dass die heutige Generation von Quantencomputern nicht mit klassischen Algorithmen mithalten kann [9].

In diesem Zusammenhang sollten die anderen, analogen Quantentechnologien nicht unerwähnt bleiben, die nicht einem universellen, digital programmierbaren Computer entsprechen, und daher hier nicht genauer besprochen werden. Stattdessen soll im Folgenden das Potenzial künftiger fehlerkorrigierter Quantencomputer im Fokus stehen, unter Einbeziehung zusätzlicher Kosten wie der Quantenfehlerkorrektur und anderen praktischen Einschränkungen.

Fehlerkorrigierte Quantencomputer

Für die Umsetzung des Quantengattermodells muss eine gewisse Redundanz in der fehleranfälligen Quantenhardware vorliegen, die Routinen zur Quantenfehlerkorrektur ausnutzt. Diese Methoden bauen aus vielen leicht fehlerbehafteten physikalischen Qubits sogenannte logische Qubits auf, die dann perfekte logische Rechenoperationen ausführen können. Effiziente und an die verwendete Hardware angepasste Routinen zu finden, ist derzeit ein stark bearbeitetes Thema in der Quantenindustrie; grundsätzlich braucht es signifikant mehr physikalische Qubits, um fehlerfreie logische Qubits zu erhalten.

Obwohl die Quantenfehlerkorrektur theoretisch gut verstanden ist, liegt bisher experimentell keine allgemein skalierbare Form vor. Für die Zukunft lässt sich sagen, dass die Quantenfehlerkorrektur die Anzahl von physikalischen Qubits und Quantengattern signifikant erhöht, damit ein Quantenalgorithmus fehlerfrei arbeitet. Um abzuschätzen, für welche Probleme die Quantenvorteile auch inklusive der Gesamtkosten bestehen bleiben, ist es von zentraler Bedeutung, Algorithmen für solche Architekturen zu optimieren und deren Laufzeit für praktisch relevante Instanzen von endlicher Größe abzuschätzen. Das erfordert detailliertere Analysen, als sie die Standard-Komplexitätstheorie liefern kann: Diese ignoriert zusätzliche Kosten und schätzt lediglich die Skalierung für asymptotisch große Instanzen ab.

Als charakteristisches Merkmal einer ersten Generation fehlerkorrigierter Quantencomputer gilt es, dass sie aus wenigen logischen Qubits bestehen und aus hardwaretechnischen Gründen eine limitierte Konnektivität zwischen den Qubits besteht, was die Parallelisierung über mehrere Quantenprozessoren nötig macht. Außerdem wird die Taktfrequenz für elementare Rechenoperationen vergleichsweise langsam ausfallen. Aufgrund dieses Mehraufwands lässt sich allgemein abschätzen, dass auch in ferner Zukunft nur die Quantenalgorithmen interessant sind, die mindestens große polynomielle Vorteile bieten [10]. Bemerkenswerterweise schließt das die meisten der bekannten Quantenalgorithmen aus [11].

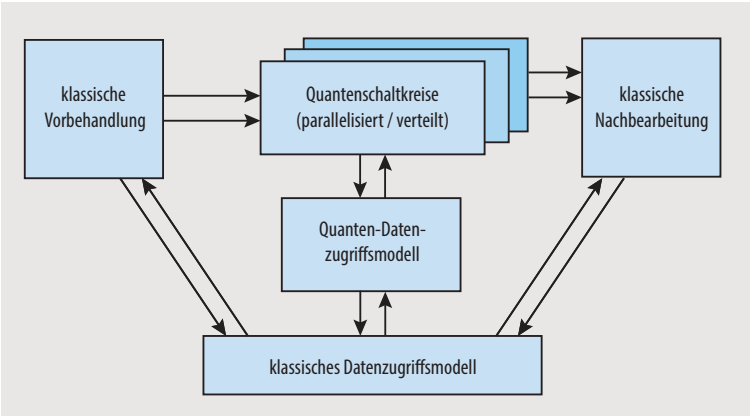


Abb. 3 Hybride Architekturen bestehen aus mehreren klassischen Bausteinen und Quantenelementen: Mit dafür optimierten Quantenalgorithmen sollen wenige Qubits für einen Quantenvorteil ausreichen.

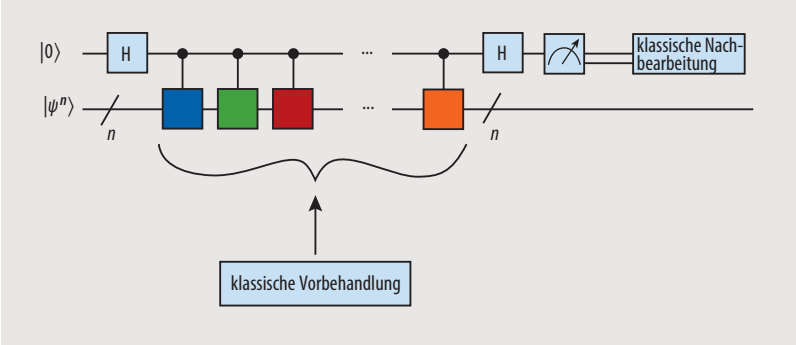


Abb. 4 Dieses Quantengatter eines randomisierten Quantenalgorithmus führt mit $(n+1)$ Qubits Operationen auf Matrizen A der Größe $2^n \times 2^n$ aus, beispielsweise die Berechnung der inversen Matrix A^{-1}, um das Gleichungssystem $A|x\rangle = |b\rangle$ zu lösen. Für das gewünschte Resultat laufen viele Runden zufällig kompilierter Quantenroutinen ab, gefolgt von intensiver klassischer Nachbearbeitung [12].

Hybride Architekturen

Um Quantenressourcen optimal einzusetzen, sollten Qubits nicht möglichst viele Schritte einer Berechnung durchführen. Im Gegenteil: Falls möglich, sollten moderne klassische Algorithmen zum Einsatz kommen und nur hochspezialisierte Subroutinen mit einem Quantenvorteil als Quantenalgorithmen ausgeführt werden. Das lässt sich effizient bewerkstelligen durch eine Kombination mehrerer parallelisierter klassischer und Quantenprozessoren sowie klassischer und quantenmechanischer Arbeitsspeicher (**Abb. 3**). Die Entwicklung sparsamer, hybrider Algorithmen quantifiziert alle gebrauchten Ressourcen, wie die Anzahl von Bits und Qubits sowie die Anzahl elementarer klassischer und Quantenoperationen (**Abb. 4**). Ziel ist es, wissenschaftlich und industriell relevante Probleme mit möglichst kleinem Quanten-Fußabdruck zu lösen und die fundamentale Frage zu klären, wann die Erweiterung klassischer Hardware mit Quantenelementen einen Vorteil verspricht.

Das konsequente Zählen aller gebrauchten Quantenressourcen macht es im Allgemeinen anspruchsvoll, Probleme zu finden, die sich bereits mit moderat leistungsfähigen, fehlerkorrigierten Quantencomputern lösen lassen. Einerseits muss es sich um Rechenprobleme mit komplexitätstheoretisch großem Quantenvorteil handeln. Andererseits muss sich dieser schon bei kleinen, implementierbaren Instanzen zeigen. Nach momentanem Wissensstand ist keine solche Anwendung in Sicht; Vielteilchensimulationen in der Physik der kondensierten Materie schneiden noch am besten ab [11]. Die für Quantenvorteile benötigte Anzahl logischer Qubits bewegt sich optimistisch geschätzt in der moderaten Größenordnung von 10^2. Aber die Anzahl logischer Rechenoperationen liegt immer noch in der Größenordnung von mindestens 10^8 [13]. Andere mögliche Anwendungen wie der Shor-Algorithmus zur Primfaktorzerlegung liegen in allen rigorosen Abschätzungen zu Quantenvorteilen noch um Größenordnungen höher [11].

Fazit

Ein bis hierher nicht angesprochener, aber wichtiger Aspekt besteht darin, dass Quantenalgorithmen in der Praxis womöglich weit besser funktionieren, als es sich momentan beweisen lässt. Diese Hoffnung ist nicht unberechtigt, wie die klassischen Algorithmen gezeigt haben, wo moderne, heuristische Methoden in der Regel deutlich besser funktionieren als jegliche theoretische, rigorose Analyse vermuten lässt. Allerdings beruhen solche Methoden typischerweise auf jahrzehntelanger Erfahrung sowie Intuition und Feinabstimmung. Häufig funktionieren sie auch konzeptuell anders als die ursprünglich beweisbar guten Algorithmen. In diesem Sinne bleibt die Hoffnung, dass stetig verbesserte Quantenhardware es erlauben wird, in den fehlerkorrigierten Bereich vorzustoßen, wo entsprechende Experimente die praktische Entwicklung von Quantenalgorithmen signifikant vorantreiben können.

In der Zwischenzeit ist es wichtig, ausreichend Expertise auf diesem Gebiet auszubilden. Es gilt, sich auf innovative Algorithmen und Anwendungsgebiete mit echtem Potenzial für Quantenvorteile zu konzentrieren – und den Schwerpunkt darauf zu legen, leistungsstarke, hybride Schemata zu entwickeln.

Literatur

[1] *R. P. Feynman*, Int. J. Theo. Phys. **21**, 467 (1982)
[2] *P. W. Shor*, SIAM Journal on Computing **26**, 1484 (1997)
[3] *F. Arute* et al., Nature **574**, 505 (2019)
[4] *J. M. Martyn* et al., PRX Quantum **2**, 040203 (2021)
[5] *Seth Lloyd*, Science **273**,1073 (1996)
[6] *S. Lee* et al., Nat. Commun. **14**, 1952 (2023)
[7] *E. Tang*, in: 51st Annual ACM SIGACT Symposium on the Theory of Computing, **217** (2019)
[8] *Z. Cai* et al., arXiv:2210.00921v2 (2023)
[9] *J. Preskill*, Quantum **2**, 79 (2018)
[10] *R. Babbush* et al., PRX Quantum **2**, 010103 (2021)
[11] *A. M. Dalzell* et al., arXiv:2310.03011v1 (2023)
[12] *K. Wang* et al., Phys. Rev. Lett. **129**, 030503 (2022)
[13] *R. Babbush* et al., Phys. Rev. X **8**, 041015 (2018)

Der Autor

Mario Andrea Berta hat an der ETH Zürich Physik studiert und dort auch promoviert. Weitere Stationen führten ihn ans Caltech und das Imperial College London. Darüber hinaus war er zwei Jahre lang als Senior Research Scientist am Amazon Web Services Center for Quantum Computing. Seit November 2022 forscht und lehrt er als Professor am Institut für Quanteninformation der RWTH Aachen und ist Visiting Reader am Department of Computing des Imperial College London.

Prof. Dr. Mario Andrea Berta, Institut für Quanteninformation, RWTH Aachen, Otto-Blumenthal-Straße 20, 52074 Aachen